

# §170.315(d)(1) Authentication, access control, authorization

**2015 Edition CCGs****Version 1.0 Updated on 10-22-2015**

## Revision History

| Version # | Description of Change | Version Date |
|-----------|-----------------------|--------------|
| 1.0       | Initial Publication   | 10-22-2015   |

## Regulation Text

### Regulation Text

§170.315 (d)(1) *Authentication, access control, authorization—*

- (i) Verify against a unique identifier(s) (e.g., username or number) that a user seeking access to electronic health information is the one claimed; and
- (ii) Establish the type of access to electronic health information a user is permitted based on the unique identifier(s) provided in paragraph (d)(1)(i) of this section, and the actions the user is permitted to perform with the technology.

## Standard(s) Referenced

None

## Certification Companion Guide: Authentication, access control, authorization

This Certification Companion Guide (CCG) is an informative document designed to assist with health IT product development. The CCG is not a substitute for the 2015 Edition final regulation. It extracts key portions of the rule's preamble and includes subsequent clarifying interpretations. To access the full context of regulatory intent please consult the 2015 Edition final rule or other included regulatory reference. The CCG is for public use and should not be sold or redistributed.

[Link to Final Rule Preamble](#)

| Edition Comparision | Gap Certification Eligible | Base EHR Definition |
|---------------------|----------------------------|---------------------|
| Unchanged           | No                         | Not Included        |

## Certification Requirements

Quality management system (§ 170.315(g)(4)) and accessibility-centered design (§ 170.315(g)(5)) must be certified as part of the overall scope of the certificate issued to the product.

- When a single quality management system (QMS) is used, the QMS only needs to be identified once. Otherwise, the QMS' need to be identified for every capability to which it was applied.
- When a single accessibility-centered design standard is used, the standard only needs to be identified once. Otherwise, the accessibility-centered design standards need to be identified for every capability to which they were applied; or, alternatively the developer must state that no accessibility-centered design was used.

### Table for Design and Performance

- [Quality management system \(§ 170.315\(g\)\(4\)\)](#)
- [Accessibility-centered design \(§ 170.315\(g\)\(5\)\)](#)

## Technical Explanations and Clarifications

### Applies to entire criterion

#### **Clarifications:**

- There is no standard required for this certification criterion.
- This criterion focuses on users that would be able to access electronic health information in the technology and not on external users that may make requests for access to health information contained in the technology for the purpose of electronic health information exchange. The latter case could require a different/additional security approach(es). [see also [77 FR 54249](#)]
- While this criterion does not specify a level of assurance, one-factor authentication would be minimally needed to satisfy this criterion. The developer has the discretion to satisfy this criterion above and beyond one-factor authentication. [see also [77 FR 54249](#)]
- A user could be a health care professional or office staff, someone who might interact directly with the technology or be software program or service. [see also [75 FR 44598](#)]

### Paragraph (d)(1)(i)

Technical outcome – A user's unique identifier(s) (e.g., username or number) is/are verified as the one claimed prior to receiving access to electronic health information.

#### **Clarifications:**

- No additional clarifications available.

**Paragraph (d)(1)(ii)**

Technical outcome – Following the user’s authentication, the technology establishes permissions associated with the user’s ability to access electronic health information and the actions the user is permitted to perform with the technology.

***Clarifications:***

- No additional clarifications available.

Content last reviewed on June 22, 2020